GAINING AND MAINTAINING CYBERSPACE SUPERIORITY: QUEST FOR A HOLY GRAIL?

BY

MERNA H. H. HSU

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Gaining and Maintaining Cyberspace Superiority: A Quest for the Holy Grail?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School Of Advanced Air And Space Studies Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Controlling cyberspace as a military domain is a challenge that demands critically assessing issues, questions, and assumptions, especially those at the foundation of the militarys decision making for operations and requirements. This thesis examined whether cyberspace can be held in like manner to existing mediums. A brief survey of classical control theories for the land, maritime, and air domains, with the intent of identifying the basic framework and its key areas of emphasis, revealed several common elements in domain control. Strategies by classical theorists, such as Halford Mackinder and Nicholas Spykman for land-centric theories; Alfred Thayer Mahan and Julian Corbett for maritime control theories; and William Billy Mitchell and J. C. Slessor for the air domain, relevantly can inform present-day and future cyberspace theorists and war planners. Given the nature of the cyberspace medium and the denominators common to controlling other domains, the US can gain and maintain cyberspace superiority. Cyberspace can be controlled in ways analogous to land, sea, and air domains. Denominators common across the classical control theories for air, land, and sea exist and are applicable to cyberspaces attributes as a dimension of war. Cyberspace control is not a Holy Grail.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**66**	

APPROVAL

The undersigned certify that this thesis meets masters-level standards of research, argumentation, and expression.

_____

Dr. John B. Sheldon (Date)

_____

Dr. James M. Tucci (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Merna Hsu received her commission from the United States Air Force Academy in 1996. Graduating from Undergraduate Space and Missile Training at Vandenberg AFB, CA in 1997, she went on to serve in missile operations at F.E. Warren Air Force Base, WY. Maj Hsu then worked in missile warning and space surveillance operations at Clear Air Force Station, AK. Following that assignment, Maj Hsu was selected as detachment commander for the 21st Space Wing's GEODSS Detachment 1 on the Army's White Sands Missile Range, NM. After graduation from Air Force Weapons School in 2003, Maj Hsu served as Chief, CAOC Space Cell; Deputy Chief, Special Technical Operations; and space weapons officer supporting Operations Iraqi Freedom, Enduring Freedom, and operations in the Horn of Africa. She then served at Headquarters Air Force Space Command at Peterson AFB, CO, in the Plans and Requirements Directorate (HQ AFSPC/A5), as a Command Lead for several space control programs and for Air Force TENCAP. She is a graduate with master's degrees from the University of North Dakota and from Air Command and Staff College. Maj Hsu hails from the great states of Pennsylvania, New York, and Hawaii. She and her family consider Alaska home.

ACKNOWLEDGEMENTS

My first thanks are for the SAASS family—faculty, staff (especially Ms. Sheila, Ms. Kelly, Grady, and our library support), and the irrepressible Class XVIII. This team continually challenged me to think more critically about the world and helped mature my ideas regarding this topic.

Significant thanks go to my thesis advisor, Dr. John Sheldon, among whose Herculean tasks was the role of guiding me in developing multifarious ideas and observations into something potentially useful. Our discussions helped me understand both the breadth and depth of the question I had hoped to answer and provided navigational assistance as I wend through the thicket of information amassed. Special thanks also go to Dr. James Tucci for his assistance in refining this product. Drs. Sheldon and Tucci were instrumental helping sculpt a product that not only communicated my ideas, but was ultimately more readable. Interacting with this team of scholar-coaches constituted a highlight in my thesis-writing experience.

Most importantly, I thank God for the opportunities and challenges this year presented. I am also deeply indebted to my family and friends, who sacrificed countless hours on the telephone and in travel to support me with their wisdom, thoughtfulness, and good humor. To this collective ohana, I owe much of the motivation that sustained me during this endeavor.

ABSTRACT

Controlling cyberspace as a military domain is a challenge that demands critically assessing issues, questions, and assumptions, especially those at the foundation of the military's decision making for operations and requirements. This thesis examined whether cyberspace can be held in like manner to existing mediums. A brief survey of classical control theories for the land, maritime, and air domains, with the intent of identifying the basic framework and its key areas of emphasis, revealed several common elements in domain control. Strategies by classical theorists, such as Halford Mackinder and Nicholas Spykman for land-centric theories; Alfred Thayer Mahan and Julian Corbett for maritime control theories; and William "Billy" Mitchell and J. C. Slessor for the air domain, relevantly can inform present-day and future cyberspace theorists and war planners. Given the nature of the cyberspace medium and the denominators common to controlling other domains, the US can gain and maintain cyberspace superiority. Cyberspace can be controlled in ways analogous to land, sea, and air domains. Denominators common across the classical control theories for air, land, and sea exist and are applicable to cyberspace's attributes as a dimension of war. Cyberspace control is not a Holy Grail.

CONTENTS

Chapter 1

Introduction

US national power and security depend on our ability to access and use the global commons. As such, the Department [of Defense] seeks the ability to achieve superiority in military-relevant portions of cyberspace.

Department of Defense
Quadrennial Roles and Missions Review Report 2009

Make no mistake: if we cannot dominate in cyberspace, we place air and space dominance at risk.

Major General William T. Lord

Despite the common critique that the United States military is a bureaucratic colossus far too slow and reactionary when adapting to confront new challenges, the Department of Defense (DOD) is moving swiftly in recognition of, and mobilization for, warfare in the cyberspace domain. As Martin Libicki points out, "Since the 1990s, when cyberspace came to the attention of DoD as a potential medium of conflict, actions in it have been considered part of a broader topic, information warfare."[1] Information warfare and information operations, however, have long existed in warfare writ large. The fresh challenges are the notions of a cyberspace domain, cyberspace operations, and cyber warfare.

From the grand strategic level of US national leadership to the military strategic levels of the DOD and its armed forces, there is a rapidly spreading recognition that warfare has expanded into yet another domain. In 2008, top civilian and military leadership standardized the

[1] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 11.

DOD's definition of cyberspace operations as: "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[2] The military continues to expand and refine its language to span cyberspace as a warfighting domain.

Additionally, the DOD has also identified what it believes to be the basic traits of the cyberspace medium. The US military has accepted that, as with other domains of conflict, cyberspace both shares, and bears its own distinct, attributes. Colin Gray astutely observes, "In common with the land, sea, air, and space environments, the electronic realm of cyberspace is a [designated] combat zone…'[C]yberspace' is [another] 'geographical' zone for…strategy to be considered."[3]

One key contrast with the other geographical environments, however, is that in embracing the idea of cyberspace as a combat zone, the military must learn how to transition from treating it as a concept to cognitively transforming it into a domain upon which to wage war. The military will have succeeded in this endeavor when it can effectively apply strategy, doctrine, and tactics to warfare in cyberspace. Only then, can the DOD claim to have fully adapted to cyberspace as a warfighting domain. Thus, the US military has yet to reach this essential point in its efforts. The DOD, however, is gaining momentum. The first major hurdle, recognizing cyberspace as a domain, has been cleared.

As of 2008, the DOD defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and

[2] Vice Chairman Joint Chiefs of Staff, "Definition of Cyberspace Operations Action Memo for Deputy Secretary of Defense," (September 29, 2008), 1.
[3] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 268.

embedded processors and controllers."[4] Within the US defense establishment, the Air Force added the ability to prevail in cyberspace to its official mission statement, formally elevating the domain and its related combat challenges to the priority of a service-level core competency in 2005.[5] Both DOD-level and Air Force senior leadership acknowledged the growing military dependency on cyberspace-related capabilities, such as information technologies (IT), and the cyberspace operations conducted in this medium.[6] In fact, the Air Force already perceives cyberspace operations and freedom to function in the domain as critical to its mission accomplishment in the air and space mediums. According to Major General William Lord, then commander of the Air Force's Cyberspace Command (Provisional) "The Air Force can neither afford unnecessary collateral damage caused by negation of our cyber capabilities nor can we achieve victory on the battlefield without cyber dominance."[7] Put simply, by 2005, the Air Force had surpassed mere acceptance of cyberspace as a domain. Cyberspace was a medium for combat, which military dominance, or command in classical military parlance, must be asserted. This significant conclusion about cyberspace now warranted overt service re-organization and proclamation by flag-rank leaders.

Little doubt now exists that the DOD and at least one of its services are already mobilizing for a deliberate approach to organizing, training, and equipping for warfare in cyberspace, or cyber warfare. That the US military be capable of achieving military superiority—perhaps even dominance or command—in cyberspace, as it has demonstrated in other domains of warfare, is considered a necessity. The Air Force, however, as does the DOD, continues to wrestle with ensuring US

---

[4] Deputy Secretary of Defense, "The Definition of 'Cyberspace'," (May 12, 2008).
[5] Rebecca Grant, "Victory in Cyberspace," (Arlington, VA: Air Force Association, 2007), 3.
[6] Grant, "Victory in Cyberspace," 3.
[7] William T. Lord, "USAF Cyberspace Command: To Fly and Fight in Cyberspace," *Strategic Studies Quarterly* (Fall 2008): 12.

military ability to defend and exploit cyberspace. Attaining military superiority in the cyberspace domain remains for the time being an abstract concept, a goal, despite the flurry of rhetoric and re-organization.

Literature addressing cyber warfare and conflict in the information age continues to accumulate. Unfortunately, in all its quantitative and qualitative abundance, this morass of material has not satiated the DOD's quest for understanding how to prepare, prosecute, and win conflicts in the cyberspace domain. Experts from government, industry, and academia offer observations that amass to fill a spectrum whose expanse is comprised of ideas ranging from science fiction-like forecasts to prescient observations.

In fairness, cyberspace is still relatively new territory in warfare's history. Although the US Air Force and its sister services have embraced IT and exploited the electromagnetic spectrum for decades, the recognition of cyberspace as a distinct domain of warfare is relatively recent. Even information warfare, under which cyber warfare currently is a subset, has existed and been a discussion subject tracing back to Sun Tzu's era. In contrast, controlling cyberspace as a military domain is a new challenge. Nonetheless, as Colin Gray rightly concludes, "the general unfamiliarity of the concept of cyberspace, and the unknown technical and tactical terms of engagement there, is offset by the familiarity of the logic of strategy that rules that (anti-) 'geography', as it does every other one."[8]

Therefore, in the speedy search for answers on adapting to this new challenge, the military should not neglect an important area of intellectual capital investment: assessing whether it is addressing the right questions, especially those at the foundation of its strategic

[8] Gray, *Modern Strategy*, 268.

assumptions. "Slow and reactionary" must not be compounded by "presumptuous and myopic" as the key traits of a vicious cycle that could become the undercurrent of the military's adaptation for cyber warfare and efforts to attain control of this domain. In its gallant headlong rush to organize, train, and equip for combat in the cyberspace domain, the US military must not bypass the core question of whether and how this medium might be controlled. Has the US military's fundamental assumptions, upon which it now so rapidly seeks to construct a foundation adequate for achieving cyberspace superiority, been examined for validity? The military should be wary of simply assuming feasibility is a given, since other domains were tamed in the past.

Thesis and Methodology

The purpose of this thesis is to examine whether the fundamental assumption that cyberspace can be controlled in like manner to existing mediums is achievable. Can cyberspace be held or controlled in ways analogous to land, sea, and air domains? Or, has the military embarked on a quest for a Holy Grail that will forever lie beyond its grasp? The US military may be moving so quickly that it is about to stumble into the pitfall of overconfidence from past successes in controlling other domains. The DOD seems to assume cyberspace can be subdued as a domain simply because the US was able to do so in the other domains.

The methodology employs a comparison and contrast framework informed by classical control theories for the land, sea, and air domains, respectively. The approach facilitates an examination of cyberspace control feasibility that is informed by the strategies that classical control theorists have proposed for achieving superiority in the land, sea, and air domains. The US military need not start from scratch or re-invent the

wheel. In fact, the military may earn dividends by simply paying heed to what the classical control theories reveal about mastering domains.

Therefore, Chapter Two serves as a brief survey of classical control theories for each of these domains with the intent of identifying the basic framework and its key areas of emphasis. Strategies by theorists, such as Halford Mackinder and Nicholas Spykman for land-centric theories; Alfred Thayer Mahan and Julian Corbett for sea control theories; and William "Billy" Mitchell and J. C. Slessor for the air domain will be considered. Classical land, maritime, and air control theories will be examined in order to extrapolate common denominators for achieving military superiority in these domains.

Chapter Three highlights some key attributes of the cyberspace domain that are relevant when addressing the feasibility of controlling this medium. If denominators common across the classical control theories for air, land, and sea exist, then do these domain characteristics offer information useful for assessing whether cyberspace can be controlled? What does cyberspace have in common with the other domains conceptually, if not physically? These aspects of the cyberspace domain will be compared and contrasted with the characteristics of the other domains.

Chapter Four provides findings underpinning the assertion that the cyberspace domain can be controlled. Success in this endeavor, however, requires military expectations shaped by experiences in land, maritime, and air mediums, be modified to account for cyberspace's attributes. Other domains' traits should not automatically be projected onto cyberspace in order to force-fit old practices and solution sets that enabled military superiority in other mediums. The definition of domain control, or superiority, in this arena must offer latitude for military and civilian strategists to adapt and resist the tendency to mirror-image across domains.

Chapter Five presents conclusions and implications. It offers additional questions and points-to-ponder for this relatively new warfighting territory. It would be premature and a costly mistake for any decision maker to assume closure and to halt discourse—strategic, organizational, or otherwise—on any aspect of cyber warfare at this early juncture. With the significant decision to recognize cyberspace as a distinct warfighting medium, the DOD has made a choice on the route it will take at yet another fork in warfare's road. The DOD must recognize that this new path bears distinctive characteristics of its own that the military traveler must learn to heed. It differs from the road network previously traversed, although that experience should not be completely discarded as irrelevant either.

In order to determine whether cyberspace can be controlled in like manner to other domains of conflict by examining classical control theories, it is necessary to bound the discussion. The focus will aim above the techno-tactical details and tackle the subject of superiority in the cyberspace domain at the strategic level, which the DOD has yet to demonstrate an adequate investment of attention. It also precludes discussion of inter- and intra-organizational challenges. Although technical, tactical, and organizational aspects of the DOD's cyberspace challenges significantly will influence the military's efforts to formulate its strategy, doctrine, and tactics for cyberspace operations and cyber warfare, in general, they remain outside the scope of this discussion. The military already is wrestling with these issues, some of which qualify as wicked problems.[9] What the military must also contend with, sooner rather than later, is regularly examining fundamental questions, answers, and assumptions.

To be sure, the military cannot and should not dawdle before it adapts to confront the rising instances of hostile cyber activity. It cannot

[9] Horst Rittel and Melvin Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4 (1973): 160.

wait for every question, answer, or assumption to be addressed comprehensively; complete knowledge is an illusion. Already, cyber threats are not mere conjecture. Public awareness on conflict in the cyberspace domain will only heighten over time, although sensitivity and tolerance to cyber attacks may vary depending on the degree of disruption to safety, security, and daily convenience. Any inventory of hostile cyber activity to date includes both small and large-scale attacks with differing levels of impact and tactical sophistication.

Moreover, cyber attacks have become prevalent as state and non-state actors strike their adversaries in and through this domain. State actors, such as China, Russia, and Israel have condoned, if not unofficially sanctioned, their citizenry and sympathizers' cyber attacks on entities perceived as antagonistic to their respective national interests. Non-state actors, such as terrorist groups and private individuals, motivated by nationalism, ideology, or criminal volition, have learned to exploit cyberspace as a means of bolstering their advantages in asymmetric assaults on nation-states. For the US and its allies, the Global War on Terror (GWOT) has already expanded into the cyberspace domain. For the GWOT and other reasons, the US military is right in concluding there is a need for cyberspace superiority, but it risks failing to achieve that objective by allowing potentially faulty or unvalidated assumptions to form the basis of its decisions and plans.

Chapter 2

Checking Six: From the Past, the Future

The short answer is that the coming of "third wave" or information age warfare…even if the new phenomenon delivers much of what its prophets advertise—the desirable and the undesirable—simply adds fresh material for explorations in strategy. It matters not to the strategist whether the subject is stone-age warfare, industrial-age warfare, or now information-age warfare.

Colin Gray

We are not talking about battles; we are talking about war. There are plenty of books and there is plenty of good understanding on battles and even on series of battles. But there is precious little study and understanding of the patterns they form and the plans and concepts that they are a part of.

Rear Admiral J. C. Wylie

Although cyberspace superiority involves a relatively new medium, the concept of controlling a domain is not bereft of theoretical and practical precedents. The intent for this chapter is a comparison of some influential and better known classical domain-centric theories, such that recurring themes might be inferred and freshly applied to strategic thinking regarding cyberspace control. Extrapolating some common elements from these past theories pertaining to achieving superiority in each geographical domain, space excepted, informs this paper's determination of whether present notions of military superiority remain intact for cyberspace. That is, whether cyberspace superiority can be construed, and consequently achieved, in a manner similar to the control of other domains.

Just as a theory can be a *succes d'estime*, a theory can earn well-founded criticisms or generally lose practical support due to the polemic manner in which a theorist advances propositions. While a number of theories may be considered tainted in this manner, they are nonetheless included here because they have theoretical underpinnings that still hold merit and concepts that are useful to this discussion. Moreover, to focus succinctly the scope of this paper, only two theorists per domain, along with elements fundamental to achieving superiority in their respective domains, are presented, understanding that this distillation necessarily reduces each theorist's argument to salient elements, such as the main proposition and its key areas of emphasis.

The survey of classical theories for each of these domains begins with Halford Mackinder and Nicholas Spykman for the ground-centric perspective. Alfred Thayer Mahan and Julian Corbett's respective maritime theories follow. Next, William "Billy" Mitchell and J. C. Slessor's works regarding controlling the air domain are briefly addressed. The chapter then concludes with an extrapolation of themes common to these various theories. These common elements later apply as criteria with which to assess cyberspace control feasibility under the current rubric of domain superiority.

Land Domain Theories

Halford Mackinder's Heartland Theory

Halford Mackinder's theory of the heartland presents a concept of achieving control across the ground domain, or land superiority, from a world system perspective.[1] Although there are criticisms ranging from alleged influence on German politics, because the concept was extolled

[1] Halford J. Mackinder, "The Geographic Pivot of History," in *The Scope and Methods of Geography and the Geographical Pivot of History: Reprinted with an Introduction by E.W. Gilbert* (London: William Clowes and Sons, Limited, 1951), 10-11.

by German leaders during World War II, to the author's revisions to the heartland's boundaries, this theory nonetheless offers an insightful perspective on domain control. Even with added concerns of invalidation given the advent of airpower, Mackinder's theory regarding gaining control over the various land regions, from a world system vantage point, is still useful.

As the 19th century drew to a close, the 400-year period of European overseas exploration and conquest abroad—the Columbian epoch—was ending.[2] As a result, it was necessary to view the world as an enclosed environment, one in which activities in any one area inevitably had consequences that would reverberate throughout this system. He labeled the most important region the pivot area, a strategically important heartland territory whose controller would wield considerable power over all remaining lands.

With the expansionism of the Columbian era waning, nation-states would begin cultivating and capitalizing on resources—environmental and human—in the territories they occupied.

> With very little of the world left to conquer, "every explosion of social forces" would take place in a much more enclosed environment and would no longer be dissipated into unknown regions; efficiency and internal development would replace expansionism as the main aim of modern states.... This being the case, ...it was important to consider what the future would bring to the great strategical 'pivot area' of the world—central Russia.[3]

More importantly, Mackinder concluded that by the early 20th century modern means of transportation, such as railroad networks, and communication had ostensibly begun transforming the world's continents into mere islands.[4] Mobility of people and resources—raw

---

[2] Mackinder, "The Geographic Pivot of History," 30.
[3] Paul M. Kennedy, *The Rise and Fall of British Naval Mastery* (Malabar, FL: Robert E. Krieger Publishing Company, 1982), 183.
[4] Halford J. Mackinder, *Democratic Ideals and Reality: A Study in the Politics of Reconstruction* (New York: Henry Holt and Company, 1919), xxiii.

and processed—had closed the spatial distances that once diluted the impact territorial resource abundance and population capability. States that placed agency in arenas, such as naval power, over controlling land that bore resource potential jeopardized their security within the international system. Paul Kennedy understood Mackinder's theory as a clarion call for states whose power and security rested primarily in the capacity for maritime superiority. Mackinder was predicting "the rise of certain super-powers with massive populations and industrial and technological strength."[5]

Mackinder divided the earth's land regions into the World-Island and its satellites.[6] These satellites were deemed lesser islands, comprised of lands in the Inner or Marginal Crescent and those in the Outer or Insular Crescent.[7] Europe, Asia, and Africa constituted the World-Island, where the pivotal Heartland lay in its center. The Inner Crescent included Germany, Austria, Turkey, India, and China.[8] Britain, South Africa, Australia, the United States, Canada, and Japan comprised the outer crescent.[9]

Mackinder asserted the nation or entity that controlled the Heartland would be the pivot state that controlled the vast majority of the world's resources. He summarized his heartland theory by stating, "Who rules East Europe commands the Heartland: Who rules the Heartland commands the World-Island: Who rules the World-Island commands the World."[10] Mackinder explained that, "the oversetting of the balance of power in favour of the pivot state, resulting in its expansion over the marginal lands of Euro-Asia, would permit of the use

[5] Kennedy, *The Rise and Fall of British Naval Mastery*, 184.
[6] Mackinder, *Democratic Ideals and Reality: A Study in the Politics of Reconstruction*, 67-69.
[7] Mackinder, "The Geographic Pivot of History," 42.
[8] Mackinder, "The Geographic Pivot of History," 43.
[9] Mackinder, "The Geographic Pivot of History," 43.
[10] Mackinder, *Democratic Ideals and Reality: A Study in the Politics of Reconstruction*, 150.

of vast continental resources for fleet-building, and the empire of the world would then be in sight."[11]

Key Factors. Critical to effective domination of the Heartland—an expanse of territory bearing the majority of the world's resources, environmental and human—and to the subsequent ability to command the land domain writ large were a number of factors Mackinder described as, "relative number, virility, equipment, and organization of the competing peoples."[12] Put simply, population—manpower and capability—and industrial capacity, along with the mobility necessary for movement of these goods via lines of communication were keys to leveraging the potential of the Heartland as a springboard for world land domination.

These essential elements are implicit in Mackinder's observation of how the Russian Empire, whose territory included much of the Heartland during his day could achieve land superiority as the potential pivot state:

> [T]he Trans-Siberian railway is still a single and precarious line of communication, but the century will not be old before all Asia is covered with railways. The spaces within the Russian Empire and Mongolia are so vast, and their potentialities in population, wheat, cotton, fuel, and metals so incalculably great, that it is inevitable that a vast economic world, more or less apart, will there develop inaccessible to oceanic commerce.... Is not the pivot region of the world's politics that vast area of Euro-Asia which is inaccessible to ships, but...is to-day about to be covered with a network of railways?[13]

From Mackinder's view, an industrialized World-Island with effective lines of communication would be an unsurpassable and nearly unassailable base for global power. For Mackinder, "nations long dormant, though potentially powerful because of their populations and

[11] Mackinder, "The Geographic Pivot of History," 43.
[12] Mackinder, "The Geographic Pivot of History," 44.
[13] Mackinder, "The Geographic Pivot of History," 43.

resources, had been galvanized by the Unbound Prometheus—the impact of technology and organization—and these revolutions were already having important strategical consequences."[14] Put simply, if the pivot state, Russia or otherwise, mustered sufficient development across its social, political, and economic fronts, it could exploit the resource-rich Heartland, then the World-Island, as a natural seat of power with which to assert land control at the global level.

Nicholas Spykman's Theory

Nicholas Spykman explicitly builds from and critiques Mackinder's Heartland theory. At the conceptual level, the two theorists are fundamentally similar in their view of the land domain as a system vital to national security. Spykman was influential in his own right, though. His theory significantly affected the US's Cold War containment policy approach.

While Spykman concurs with Mackinder's concept regarding certain territory as more critical than others for achieving land control, Spykman's criteria for identifying this key region in the world system yields a different conclusion as to the pivot area. His analysis includes more specific criteria, such as topography, climate, location of production centers, and mobility. Whereas Mackinder placed emphasis on historical accounts of resource potential and anticipated industrial development potential—especially in terms of transportation and communication infrastructure—Spykman subjected his land assessments to existing infrastructure and geo-environmental trends.

Spykman organized the world's lands into slightly different regions. His theory focused on the Heartland, Rimland, and Offshore Islands and Continents.[15] Moreover, Spykman valued both land and sea power. He

[14] Kennedy, *The Rise and Fall of British Naval Mastery*, 194-95.
[15] Nicholas J. Spykman, *The Geography of the Peace* (New York: Harcourt, Brace and Company, 1944), 38-41.

credited proximity and capability to exploit the maritime domain with greater importance than Mackinder.[16] To Spykman, access to land and maritime resources was a dual strength.

Spykman also emphasized territorial size, topography, and climate—chief factors in land resource potential—as the determinants of which areas were key to land superiority. Therefore, while Mackinder concluded that this strategic area was the Heartland, Spykman considered the area he called the Rimland as the key to land domain control in the global system. To Spykman, the Rimland—lands in the area akin to Mackinder's Inner or Marginal Crescent—was the key region to control for power over the world's lands: "Who controls the rimland rules Eurasia; who rules Eurasia controls the destinies of the world."[17]

Spykman explains that Mackinder's conclusion that the Heartland, physically in the approximate area of central Russia, is not the key node for land domain control because of climate, industrial production locations, and the obstacles to mobility.[18] He points out, "The actual facts of the Russian economy and geography make it not at all clear that the heartland is or will be in the very near future a world center of communication, mobility, and power potential."[19] While the railroad and new roads could increase the mobility of resources and people in the area, the geography and climate of the region presented great obstacles. Therefore, "unless raw materials of power in central Asiatic regions of Russia turn out to be great enough to balance those of the rimland regions, Soviet strength will remain west of the Urals" and the rimland would be greater in power potential.[20] The key determinant of land superiority would be control of the Rimland.

---

[16] Spykman, *The Geography of the Peace*, 36-37.
[17] Spykman, *The Geography of the Peace*, 43.
[18] Spykman, *The Geography of the Peace*, 38.
[19] Spykman, *The Geography of the Peace*, 38-39.
[20] Spykman, *The Geography of the Peace*, 40.

Key Factors. Spykman's key factors for land's power potential encompassed and surpassed those indicated by Mackinder's Heartland theory. He acknowledged the importance of raw resources, population capability, industrial and technical capacity to process resources, and an infrastructure for mobility. Spykman, however, evaluated the potential for development in these areas with the topography and geo-environmental realities of each region.

Maritime Domain Theories

Alfred Thayer Mahan: Naval Theory

> *The methods of successive eras will differ with the character of the instruments each has.…but the factors in the hands of the opposing parties are, or should be, the same in any particular age.*[21]
>
> *Alfred Thayer Mahan*

Alfred Thayer Mahan contended that command of the sea was both possible and necessary to national security. Control of the sea provides victory in war and protection of commerce in peace. Thus, naval superiority, in support of a nation's sea power, can determine the rise and fall of nations.[22]

Key Factors. Mahan considered lines of communications, for fuel and ammunition, vital for the navy. He explained, "the most important of strategic lines are those which concern communications. Communications dominate war…. So long as the fleet is able to face the enemy at sea, communications mean essentially,…those necessaries, supplies which ships cannot carry in their own hulls beyond a limited amount."[23]

Additionally, fortified strategic harbors and strategic ports were critical since naval forces and commercial ships required bases for periodic repair and resupply. Moreover, commerce ships required designated ports for loading and off-loading of trade goods.

---

[21] Alfred T. Mahan, *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, ed. John B. Hattendorf, Classics of Sea Power (Annapolis, MD: Naval Institute Press, 1991), 152.
[22] Mahan, *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, 95.
[23] Mahan, *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, 144.

Fleet production and capability were also key, if the intent was to control the sea. In fact, the enemy's fleets—military and commercial—were the key objective for destruction. The navy must reduce or destroy the opposing navy at every opportunity. Therefore, both quantity and quality of ships were essential. To control the sea, a naval force must decisively destroy the enemy navy or default to persistently escorting commerce convoys.

Additionally, if the navy existed to protect national maritime commerce, enemy shipping should also be targeted. Mahan asserted, "Whether it comes before or after the seizure of the objective, a battle must be fought if a decisive naval superiority does not already exist; and if it does, that superiority must be energetically used to destroy every fragment of the enemy's shipping within reach."[24]

Maintaining a concentration of fighting ships would enable decisive victories during encounters with enemy ships. Mahan emphasized the need to prevent dispersing the fleet's vessels, since this would also dilute force strength needed for decisive engagements. He also advocated the use of blockades as a means to contain enemy fleet dispersion and force fleets to fight decisive battles in order to achieve naval superiority.

Julian Corbett: Maritime Theory

Julian Corbett considered naval strategy a part of an overall maritime strategy. He explained, "for a maritime state to make successful war and to realize her special strength, army and navy must be used and thought of as instruments intimately connected."[25] The navy is simply another instrument of war whose employment must be coordinated with the other branches of armed forces. The type of war—limited or unlimited—would affect operations for maritime superiority. In

[24] Mahan, *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, 196.
[25] Julian S. Corbett, *Some Principles of Maritime Strategy*, ed. Eric J. Grove, Classics of Sea Power (Annapolis, MD: Naval Institute Press, 1988), 11.

contrast to Mahan, he did not emphasize the destruction of the enemy navy for control of the sea. Corbett also did not view superiority in a binary sense of all or nothing. Unlike Mahan, he considered the object of naval warfare to be command of the sea or to prevent the enemy from securing this superiority.[26]

While his theory builds upon Mahan's concepts, Corbett considered the normal state of the sea as un-commanded, continually contested by combatants. He explained it was a fallacy to link national security to permanent command of the maritime domain since this was physically impossible and could not be legally enforced due to lack of ownership rights in international waters. Corbett concluded that command of the sea "is not identical in its strategical conditions with the conquest of territory" and that a more reasonable approach was to "inquire what it is we can secure for ourselves, and what it is we can deny the enemy by command of the sea."[27] Moreover, he equated command of the sea with control of communications and commerce—right of safe passage for trade.

Key Factors. Parallel operations, such as joint operations, to secure lines of communication would be required to achieve war's political ends. Protecting lines of communications on land and at sea was vital in the defense strategy of a nation in peace and war. Unlike land warfare, control of the sea served the purpose of controlling communications—military or commerce—rather than seizure and occupation of territory for its own sake.

Corbett subscribed to an economy of force approach, since the geographic expanse of the oceans could not be saturated with a permanent presence of ships. His approach concentrated maritime efforts on covering choke points. Controlling choke points or areas that

[26] Corbett, *Some Principles of Maritime Strategy*, 91.
[27] Corbett, *Some Principles of Maritime Strategy*, 93.

encompassed strategic lines of communications would optimize the use of finite naval assets.

Modifying Mahan's binary sea control theory, Corbett introduced variable control. Even with passive resistance by a defensive adversary, given the sea's vastness of territory compared to fleet size and speed, command of the sea could only occur for a finite period of time over specific areas. Consequently, command of the sea would usually be in dispute and could not be absolute even over small areas or short time periods.

Corbett introduced four variations of sea control. Two were spatial, general or local, and two indicated degree of effectiveness temporally, temporary or permanent.[28] General command could be permanent or temporary. Local command, however, rarely could be permanent, since it would be vulnerable to interruption even under the best of geographic circumstances.[29] More importantly, Corbett pointed out that, "even permanent general command could never in practice be absolute. No degree of naval superiority can ensure our communications against sporadic attack from detached cruisers or even raiding squadrons…prepared to risk destruction."[30]

As important, there was also a difference between exercising and securing control of the sea. Corbett saw battle fleets as a means to secure control of the sea while cruisers exercised, or enforced, control. The naval force required for gaining and maintaining superiority at sea necessarily depended on the adversary's maritime force strength. Corbett determined that securing command could be accomplished by military or commercial blockade. More traditionally, it could also entail forcing a decisive engagement—difficult if the enemy chose to disperse or evade battle due inferior naval numbers or as a means to frustrate his

[28] Corbett, *Some Principles of Maritime Strategy*, 104.
[29] Corbett, *Some Principles of Maritime Strategy*, 104.
[30] Corbett, *Some Principles of Maritime Strategy*, 105.

opponents' fleet concentration efforts.[31] Since opponents could dispute control by having a fleet-in-being or conducting small-scale counter-attacks, exercising control included defense against invasion, attack and defense of commerce, and military expeditions to maintain coercive pressure or reduce the adversary's forces.

Lastly, by refining Mahan's sense of fleet concentration, Corbett allowed for force dispersal in an area near a designated strategic center. This allowed for better exercise of control, to protect lines of communication, while creating conditions for concentrating and massing a fleet for decisive battle when needed.

[31] Corbett, *Some Principles of Maritime Strategy*, 156.

Air Domain Theories

William "Billy" Mitchell

William "Billy" Mitchell asserted that air superiority could best be achieved via air combat between pursuit aircraft. Bombardment and attack aircraft served second and tertiary roles to force enemy aircraft into aerial battle and to support ground operations.

Key Factors. Since Mitchell concluded air superiority would be achieved by forcing enemy aircraft into air-to-air battles, he emphasized destruction of adversary aircraft in the air domain. Like Mahan, he envisioned massed and decisive fleet battles. "The air force has ceased to remain a mere auxiliary service for the purpose of assisting an army or navy…. The air force rises into the air in great masses of airplanes. Future contests will see hundreds of them in one formation."[32]

Mitchell organized the air force into three branches: pursuit, bombardment, and attack.[33] Pursuit aviation is fundamental to the control of the air. He considered defeating hostile pursuit aviation a prerequisite for victory in the air domain, emphasizing, "an air force must be able to defeat the hostile pursuit aviation or everything else will fail."[34] Vital centers were important to the extent that their bombardment would compel enemy aircraft fly in order to defend them. Thus, bombing created opportunities for air combat and annihilation of the enemy air force.

---

[32] William Mitchell, *Winged Defense : The Development and Possibilities of Modern Air Power Economic and Military* (Mineola, N.Y.: Dover Publications, 2006), 8.
[33] Mitchell, *Winged Defense : The Development and Possibilities of Modern Air Power Economic and Military*, 164-65, 70.
[34] Mitchell, *Winged Defense : The Development and Possibilities of Modern Air Power Economic and Military*, 164.

Additionally, national industrial and population support were important elements for airpower and its ability to dominate the air. In *Winged Defense*, Mitchell communicated his concern that intelligence of adversary capabilities was vital to ensuring the US developed and produced the best military aircraft.[35] Keeping a technological edge over the adversary was both desirable and necessary.

J. C. Slessor

J. C. Slessor, like Mitchell, considered air superiority critical.[36] He asserted, however, that localized air superiority was achieved and maintained through both air-to-air combat, bombardment of vital centers, and could be supplemented by interdiction of logistics.[37] Less polemic than Mitchell, J. C. Slessor's theory regarding control of the air took a more balanced and joint approach.

Key Factors. While Mitchell believed air combat was the primary means of destroying the enemy air force and commanding the air, Slessor suggested both types of operations are ideal for destroying hostile aircraft. To this, he added dislocation and disruption of vital centers, such as aerodromes and logistical centers. Interdiction of lines of communication to render aircraft inoperable for want of maintenance parts and fuel were also considered effective means toward attaining control of the air domain.[38]

Like Corbett, Slessor concluded that joint operations were useful for winning wars. A combination of parallel air operations was more effective for air superiority and winning a war than focusing attention only one aspect of airpower or the military. Slessor also considered the

[35] Mitchell, *Winged Defense : The Development and Possibilities of Modern Air Power Economic and Military*, 184-86.
[36] John Cotesworth Slessor, *Air Power and Armies* (London: Oxford university press : Reprint by AMS Press New York, 1936), 66.
[37] Slessor, *Air Power and Armies*, 15, 31-32.
[38] Slessor, *Air Power and Armies*, 31-32.

complete destruction of vital centers unnecessary, focusing more on disruption and denial of lines of communication (e.g., railroads) via simultaneous operations coordinated with and in support of the other services.

Common Recurring Themes

> *The division of strategy…into maritime, continental, and air strategies [is] artificial and should be made only for the purpose of study and analysis. "In practice there is, and must be, a good deal of overlap and merging."*[39]
>
> *Rear Admiral J. C. Wylie*

> *Clear conceptions of the ideas and factors involved in a war problem, and a definite exposition of the relations between them, were in his eyes the remedy for loose and purposeless discussion; and such conceptions and expositions are all we mean by the theory or the science of war. It is a process by which we co-ordinate our ideas, define the meaning of the words we use, grasp the difference between essential and unessential factors, and fix and expose the fundamental data on which every one is agreed. In this way we prepare the apparatus of practical discussion; we secure the means of arranging factors in manageable shape, and of deducing from them with precision and rapidity a practical course of action.*[40]
>
> *Sir Julian Corbett*

Several recurring themes are apparent from the various domain-centric control theories presented. Among them are the value of industrial capacity, the need for raw resources (and therefore resource potential), existence and significance of vital centers, criticality of lines of communications, and parallel operations across multiple fronts. In some cases, a surface level comparison makes evident the commonalities. For others, extrapolation is required to link concepts from theories written at different levels of strategy.

---

[39] Joseph Wylie, *Military Strategy: A General Theory of Power Control*, Classics of Sea Power (Annapolis, MD: Naval Institute Press, 1989), xxvi.
[40] Corbett, *Some Principles of Maritime Strategy*, 7.

Industrial capacity

- Indigenous ability to conduct research, development, production, and sustainment of weapons and logistics

Requirement for resources and resource potential

- Raw materials for manufacturing war materiel or for export to raise funds needed for war, for logistics
- Includes human physical and intellectual potential and capability

Vital centers/Key nodes

- Concentrations or hubs of critical resources (e.g., aerodromes, strategic ports, cities)
- Some key elements actually earned their emphasis because they facilitated exploitation of resources in other domains. In some cases, the key elements are actually located in other domains. For example,
    - Ground-based target systems that can be affected for attaining military superiority in the air domain (e.g., targeting aircraft maintenance hangars vs. solely focusing on aircraft already in flight)
    - Strategic ports and harbors along coastlines
    - Ship building centers, rail yards, depots, and major road networks that link continental interiors to the coast/access to the sea, etc.
- Indirect avenue of control, physical occupation of the entire domain not required

Lines of communication

- For effective coordination, C2, and logistics access; to attrite or increase cost for these same elements for the adversary

Parallel operations within and across domains

- Taken together, these recurring themes seem to fit into the context of what Rear Admiral J. C. Wylie astutely described as two kinds of strategies to be used in war:

> One is the sequential, the serious of visible, discrete steps, each dependent on the one that preceded it. The other is the cumulative, the less perceptible minute accumulation of little items piling one on top of the other until at some unknown point the mass of accumulated actions may be large enough to be critical.[41]

Even with the advent of a new domain by, with, and through which a different variant of warfare can be waged, the nature and purposes of war have remained constant. To be clear, the character of war has changed, but relevant ideas from past military theories should be examined to inform both present day decision making and planning for the future. IT and recognition of cyberspace as a medium of conflict, however, have not so revolutionized warfare as to retire strategy and classical theories.

Contrary to the philosophy of those evangelizing the infectious fallacy of technology as a panacea for winning wars, strategy and strategic theories remain central to the military's ability to achieve political ends—the purpose of war regardless of domains involved. Therefore, if cyberspace superiority, or control, is important to the military's effectiveness as an US instrument of power, then the military must not neglect the classical control theories that shaped the paths to superiority in other domains of war. As the DOD seeks to understand this newfound domain, it must also actively put in check its proclivity to be enthralled with the newest spate of IT-centric concepts, terminology, and weapon systems that alter the character of war, so that decision makers account for the fact that thus far, war's nature and purpose have remained immutable.

---

[41] Wylie, *Military Strategy: A General Theory of Power Control*, 119.

Chapter 3

Some Attributes of the Cyberspace Domain

While it is wise to observe things that are alike, it is also wise to look for things that differ; for when the imagination is carried away by the detection of points of resemblance,…it is apt to be impatient of any divergence in its new-found parallels, and so may overlook or refuse to recognize such.

Alfred Thayer Mahan

There are also pitfalls for those who do not adapt sufficiently to the changing character of war.

David Lonsdale

Seek first to understand. For the military to gain and maintain superiority in this domain, understanding strategically relevant features of this fabricated terrain is necessary for a successful endeavor. Although cyberspace is an artificially created domain, it nonetheless is derived from, and governed by, physical laws associated with the electromagnetic spectrum.[1] As such, cyberspace is not wholly subject to human will and whim. Despite the powerful influence of human imagination and innovation, this domain still exhibits some constancy in its nature. This chapter, therefore addresses the question, What are key attributes comprising the nature of the cyberspace domain?

A growing volume of publications describes this domain's attributes. In 2006, the DOD implemented its *National Military Strategy for Cyberspace Operations* (NMS-CO), which described cyberspace, and its characteristics and key features. The DOD has also provided its definition of cyberspace and cyberspace operations.

[1] Gregory Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 17.

For the purpose of this paper, cyberspace is as the DOD defines it, and for our purposes is limited to the internet and global information grid that uses IT for access.[2] It does not include all the links and nodes that are part of the infrastructure that make up netcentric warfare writ large. Cyberspace is therefore defined as, "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[3]

The DOD concluded cyberspace characteristics as being:[4]

- Created, maintained, owned, and operated by public, private, and government stakeholders and exists across the globe.
- Changes when technology, architectures, processes, and expertise co-evolved to produce new capabilities and operating constructs.
- Subject to the availability of the electromagnetic spectrum.
- Allowing high rates of operational maneuver that capitalizes on decision-quality information moving at speeds that approach the speed of light.
- Enabling operations across domains.
- Transcending commonly defined organizational and geopolitical borders.
- Formed by the interconnection of information and data transmission systems, supporting infrastructure, data devices, and software and hardware applications.
- Included data "at rest" and "in motion"
- Readily accessible in varying degrees to other nations, organizations, partners, the private sector, and our adversaries.

[2] Chairman Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations (U)." ((Secret) Information extracted is unclassified.), ix.
[3] Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations (U)." ix. (Secret) Information extracted is unclassified.
[4] Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations (U)." 3. (Secret) Information extracted is unclassified.

- Formed the foundation of the information environment.

According to the DOD, key features of the cyberspace domain were:[5]

- Man-made domain
- Technical innovation
- Volatility
- Information movement
- Speed

While the 2006 DOD strategy document lists domain characteristics and features that comprise the current official view of the cyberspace medium, they are not the focus of this chapter. The DOD's conclusions, however, usefully inform this discussion. They indicate the military's contemporary perception of cyberspace and serve as a point of departure for discussion. Consistent with the Secretary of Defense's expectations to "remain flexible as our understanding of cyberspace grows and our capacity to conduct cyberspace operations increases," the NMS-CO's descriptions are, therefore, considered neither complete nor incontestable. Moreover, this chapter centers on attributes that should remain salient despite inevitable progression and evolution of technological capabilities and military tactics, techniques, and procedures.

Some essential traits inherent in the nature of this medium, even as technological innovation evolves the character of warfare in cyberspace, include:

- Multi-dimensional
- Interconnected hardware and software network
- Artificial
- Technology-dependent

[5] Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations (U)." 4. (Secret) Information extracted is unclassified.

- Dynamic and Regenerative
- Opaque

Multi-dimensional

Cyberspace is both non-geographic and trans-geographic. To borrow a term from Colin Gray, it is an anti-geography.[6] Cyberspace's utility lays, in part, in its inherent ability to transcend physical domains. Others, such as Martin Libicki, have described this trait as ubiquitous.[7] The hardware and software infrastructure that is necessary for the access, connectivity, and activity in cyberspace exists on land, at sea, in the air, and in outer space. IT links and nodes are located in buildings, vehicles, onboard aircraft, relayed via spacecraft, and at sea on ships. Cyberspace exists in and across any combination of these domains simultaneously, so long as electricity and signal connectivity is available.

Further, while sea and air domains can also permeate across political boundaries, these can be and have been bounded, albeit sometimes vaguely or selectively recognized due to nation-state disputes. Aeronautical charts and nautical show territorial borders set by nations. Cyberspace's dynamic and opaque nature precludes natural or geographic boundaries, much less political lines of demarcation. This trait is unique for cyberspace, since it is also a consequence of the simultaneity of its existence across multiple countries and geographic domains.

Interconnected hardware and software network

The cyberspace domain is impeded only by lack of connectivity (e.g., physical terrain that obstructs radio waves or landlines). The extent to which connectivity is blocked can be said to form the boundaries of cyberspace. Without connectivity, users simply have

[6] Gray, *Modern Strategy*, 267-68.
[7] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 14.

activity localized to software and hardware infrastructure at hand, such as a laptop computer's operating system. Access and activity in the cyberspace commons is lost until connectivity is restored. It is the connectivity, the numerous electromagnetic lines of communications that weave to form the environmental fabric of cyberspace. Connectivity also allows these lines of communications to access content that is stored in the hardware and software infrastructure of cyberspace, such as databases and websites.

Hence, infinite, or as much as existing technology will allow, numbers of literal lines of communication comprise cyberspace. Not all lines of communication, however, are initially equal in significance to national security. Lines of communications link to different nodes, manifested in hardware and software. These lines are thus indirect relays or avenues of direct access for information exchange and system control.

Collateral effects of any activity are therefore ostensibly indeterminate. They are hard to localize due to the vastness of interconnections across domains. Even a precision strike, such as one directed at one computer IP address or server, can have physical and non-kinetic effects that cascade across levels of impact and extend to various sectors of society.

Moreover, these hardware and software links and nodes form the backbone of cyberspace's vast reach of coverage. Concentration points in terms of servers, data bases, antennae relay towers, satellite bent pipe architectures, extend lines of communication within and across domains at high speed. Deliberate interference, electrical impedance, hardware and software processing capacity, and glitches are its few brakes.

Artificial

The artificiality of cyberspace as a domain is obvious. It is a manufactured environment, even if the electromagnetic spectrum is

natural and pre-existing. Since the medium is manufactured, cyberspace is malleable and fluid—evolving and expanding at the speed of software and hardware innovation. Cyberspace's rules and processes, (e.g., operating protocols), have wide latitude for evolution since they are bounded only by the physical laws governing the electromagnetic spectrum, such as bandwidth availability.

Presence and displacement are not physical, except at electron level. Computer network attacks, borrowing a page from electronic warfare, would repel or overrun adversaries' only in the sense that one tactic might be to blast a continuous stream of hits or electrons at a website, network port, or computer IP address. Military tactics, techniques, and procedures must be translated to this artificial domain by new terms and concepts.

Technology-dependent

Presence and activity in cyberspace require technology. As an artificial domain, technology is mandatory for access, activity, and control. Electricity (and all its electrons) is the lifeblood of the domain. All users require an infrastructure or access to infrastructure in order to enter cyberspace. Like outer space, technology is necessary for presence and activity. Unlike the other domains, however, neither hardware nor software can physically occupy a place in cyberspace.

Yet, despite the need for technology as a key to unlock the gates to cyberspace, this entry is low cost due to the proliferation of commercial products and services competing for profit. Barriers to entry can be easily scaled, so long as the user environment has access to electricity and basic electronic hardware and software. The ease of access is particularly significant since entrants are able to traverse multiple domains once connected to cyberspace.

Dynamic and Regenerative

With its links-and-nodes, cyberspace dynamically expands, contracts, and readily regenerates from hostile activities among its users. Cyberspace is repairable and reconstituted to the extent that there is redundancy of capabilities (other lines of communication or server) that can be connected when others are taken off-line voluntarily or involuntarily due to attack or malfunction.

The content resident at vital centers, such as nodes, and in transit on millions of lines of communication can also be dynamic and regenerative by way of redundancy via file duplication or copied onto back-up storage locations. Unknown quantities of copies of files or websites can migrate to other servers (e.g., Georgia's government websites migrating to a commercial company's servers in Georgia in the US).[8] Cyberspace and its contents are not bound by physical limitations.

Opaque

Except for its hardware infrastructure, cyberspace is intangible to human senses. Activity is inherently veiled, masked, or otherwise obscured by cyberspace's vastness and dynamic boundaries. Like the maritime environment, it may be impossible to discern all activity, much less identify and halt hostile operations, without negating all activity, such as through an EMP blast or nuclear strike over a physical locale. Even then, this denial is localized and temporary to the immediate physical domains in range of the attack's effects. Moreover, deception of level-of-attack damage is easier to hide or minimize, relative to verifying and measuring damage. Anonymity is the default status, unless a legal regime imposes cyberspace protocols that are enforceable.

[8] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* Winter 2008-2009 (2009): 66-67.

Recognition of an environment's attributes aids effective adaptation for exploitation and control. The military seeking to attain superiority in the cyberspace domain should comprehend the strategically salient features of this artificial terrain. Mapping these basic parameters of the nature of cyberspace as a domain renders this battle space more tractable for asserting control.

Chapter 4

Findings

The Cyberspace Superiority Grail: Choosing Wisely

Cyberspace has become an arena where various actors struggle for dominance. The signs have been around for years.

Rebecca Grant

Our approach to cyberspace must remain flexible as our understanding of the domain continues to mature, and as US, alliance, coalition partners, and adversary capabilities to operate in cyberspace increase. The Department [of Defense] remains steadfast in our commitment to achieve superiority in the military-relevant portions of cyberspace.

Department of Defense
Quadrennial Roles and Missions Review Report 2009

Command does not have to be either "total" or "permanent."

David Lonsdale

According to the Secretary of Defense, the DOD's reliance on cyberspace renders this domain an avenue of exploitation for adversaries to gain strategic, operational, and tactical advantages over the US.[1] Not only is cyberspace useful for the capabilities within the domain, the military (and other instruments of national power) increasingly rely upon cyberspace for essential support to operations in other domains. The DOD's consequent commitment to securing cyberspace soon manifested in the recognition of this artificial dimension as another domain for war. This spurred the armed services and government agencies to apply a

[1] Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations (U)." v. (Secret) Information extracted is unclassified.

cognitive framework that treated cyberspace as a dimension of warfare co-equal to the four geographic mediums. Similar rhetoric and reorganization that accompanied previous recognition of other dimensions for warfare, such as air and space, ensued.

The Department of Defense developed *The National Military Strategy for Cyberspace Operations*. The document "describes the cyberspace domain, articulates threats and vulnerabilities in cyberspace, and provides a strategic framework for action" and "is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain."[2] Military strategic superiority required "ensuring our own freedom of action in this contested domain while denying the same to our adversaries."[3] The 2009 *Quadrennial Roles and Missions Review Report* further refined the military's areas of focus by stating that the DOD stood by its commitment to achieve superiority in the military-relevant portions of cyberspace.[4]

In this quest for the Holy Grail of cyberspace control, the military should take care to question its assumptions, especially ones so fundamental and upon which further questions and answers are predicated, lest it build a foundation on shifting sand. Tackling cyberspace superiority is not a wholly new challenge. There is practical knowledge to be gleaned from classical theories from other domains. While the US military should be wary of simply repeating or superimposing these past strategies on cyberspace as templates, it is instructive to examine the manner in which control over other domains have been asserted.

---

[2] Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations (U)." vii. (Secret) Information extracted is unclassified.
[3] Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations (U)." v. (Secret) Information extracted is unclassified.
[4] Department of Defense, "Quadrennial Roles and Missions Review Report," (January 2009), 18.

The military will not have embarked on a quest for a Holy Grail that will forever exceed its reach, if it is careful in choosing the true Grail. If the DOD, however, misidentifies the Grail—assuming that cyberspace superiority will be achieved and defined just as control is over land, maritime, and air domains—the military will have chosen poorly. For example, denying enemy freedom of action by simply superimposing the "if it flies, it dies" concept from air superiority-centric approaches to domain control may not be feasible. The DOD's recent rhetoric belies this proclivity readily to recycle buzz words and phrases without validating whether the terms are appropriate. Worse, some quarters lurch to the other extreme, convinced of the need to reject all existing concepts for the sake of responding to a revolution in warfare.

Neither swagger fueled by poorly reasoned optimism from past successes in other domains, nor disdain for past experience as antiquated and therefore automatically obsolete, is wise. While rhetoric incorporating familiar terms (e.g., dominance, superiority) is necessary to galvanize a constituency for cyberspace and to provide context for the inherent advantages and challenges it brings to the character of war, the DOD can go overboard. Momentum can cause organizations to bypass critical analyses informed by theory and grounded in evidence and experience. Recycling past concepts can be useful, when judiciously done.

Moreover, if the DOD is overly ambitious in its requirements for control, mistaking wants for requirements, its greedy swagger will be evident as cyberspace operations become reactionary and restrictiveness supersedes utility. Consequently, the military will be frustrated in its efforts, or worse, have fooled itself into believing it has attained cyberspace superiority, when, in fact, it has fallen short and ceded the asymmetric advantages this domain affords to those who can hold an egg without crushing it. Ends and means must be accurately understood for proper ways to be developed to bridge the two. For cyberspace

superiority, the challenge is amplified because the means seem to change with the pace of IT innovation, and the ends are easily misidentified.

Cyberspace Superiority: Recognizing the Grail

If military superiority in a domain is defined as freedom of action and the ability to deny the same to adversaries, then cyberspace superiority—particularly when focused on military-relevant portions of the domain—is achievable. As significant, cyberspace superiority may be gained and maintained in a manner that exploits aspects significant to controlling the other mediums. Therefore, considering the commonalities that emerge from surveying classical control theories and a strategic - level view of cyberspace's topographical attributes, the US can seize the cyberspace superiority Grail. The recurring themes from the classical control theories examined offer theoretical factors for consideration when developing a strategy for achieving military superiority in a domain. The nature of cyberspace is such that these factors can be effectively exploited to advance control of this domain. It follows that, at least from the perspective of classical control theories, there are sufficient commonalities that render control of cyberspace tractable via some of the same mechanisms leveraged for controlling the other domains.

Given the military's usage of cyberspace, grasping the superiority Grail requires the ability to ensure authenticity of content in and from cyberspace, and reliable access to this domain. At minimum, military strategy, operational planning, and tactics involving cyber operations require that these essential capabilities exist to some degree. Moreover, the ability to deny these capabilities to adversaries must be available at the time and place needed to support military operations, whether in cyberspace or other dimensions.

Permanent control over the entirety of cyberspace, such as Mahan's concept for sea control, which Julian Corbett later categorized

as general control, is not a requirement, but a greedy hope.[5] Temporary, localized or area control, when and where needed, however, is essential.[6] Permanent, or even temporary, general control for all of cyberspace would be tantamount to wielding a weapon of mass destruction, or weapon of mass effect (e.g., a nuclear or other electromagnetic pulse device), due to the widespread and indeterminate collateral effects following execution. The capability for such a widespread and absolute degree of control for this domain may one day be technologically possible, but the impact of such a weapon capability would render its use a social taboo for any situation short of national survival. Like nuclear weapons, such a capability would be of great deterrent value, but rarely used operationally. Its use would result in a pyrrhic victory given the political, social, and economic ramifications involved. Thus, disruption, or temporary denial, of adversary freedom of action offers a more flexible, albeit still intelligence-intensive, and pragmatic option for superiority in cyberspace. Moreover, it meets the intent of military superiority in a domain.

A more specific form of control pertains to assuring access, which is essential to freedom of action. It complements assurance of information authenticity and protects against other types of adversary activities that reduce our advantage in cyberspace. Access to content and lines of communication sufficient, that is timely and reliably, for effective operations, such that planning and actions can use cyberspace is also a requisite for cyberspace superiority. Without these linkages, there is no interconnectivity. Random disruption or unreliable access will deter planners and operators from using cyberspace. Control of a domain must include access to it, so that control might be exercised and

[5] Reference *Some Principles of Maritime Strategy* by Julian Corbett for more details regarding his concepts for maritime control.
[6] Reference *Some Principles of Maritime Strategy* by Julian Corbett for more details regarding his concepts for maritime control.

enforced. Thus, to lose reliable access is to give up any notion of plausible control of a medium.

With assurance of authenticity and access, the military can achieve a primary requirement of cyberspace superiority, namely freedom of action, to the degree that military operations may dependably use cyberspace capabilities. Given that hardware, software, and the information in, or transiting, the interconnected IT infrastructure form the military-relevant aspects of cyberspace, authenticity assurance means security from tampering or interception. Whether information—the manifestation of materiel and resources in this domain—is resident in vital electronic storage centers, or in transit via lines of communication (e.g., land lines or electromagnetic waves), there must be verifiable proof that the data, was uncorrupted and unhindered (e.g., temporarily intercepted for file copying, then re-transmitted) from the point of transmission to receipt.[7]

Loss of data may be easier to discern due to lack of receipt. Pirated data, however, may be information that was copied and relayed to unintended recipients, while the intended recipients remain oblivious, since they still received their expected information. This is still tantamount to lost or intercepted goods because information involuntarily siphoned is now available to adversaries, who also benefit from the potential advantage held by the sender and intended recipients. As Libicki noted, the value of information is affected when compromise is real or perceived.[8] Loss, in this case, is measurable in information advantage lost or gained. Confidence in the security and veracity of information on or traveling through cyberspace is part and parcel of cyberspace superiority.

Moreover, assured freedom of action reflects an implicit defensive or protective capability to deny adversary access to military-relevant

[7] Author discussion with Dr. Stephen E. Wright, November 2008.
[8] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 23.

areas of cyberspace, such as .mil accounts and classified portions of US government-created cyberspace. Denial of freedom of action for adversaries must, at a minimum, include defense of these cyberspace perimeters. Access into these electronic areas of operations is akin to allowing adversary vessels and pirates to loiter unchallenged in the vicinity of the US coastline. Active and passive activity by unfriendly states and non-state actors must be deflected to the extent that the US is aware of their presence or activity. While it may not be possible to stop every IP ping (which may be accidental) or probe, the DOD must control access to such an extent that unauthorized entities are unable to copy, block, or alter information contained within areas of cyberspace formed by government networks. Cyberspace situational awareness is an essential capability for assuring the authenticity of military cyberspace content.

Just as certain segments of the US coastline are afforded more patrols and fortifications due to their economic importance or the strategic ports and harbors in that locale, military-relevant portions of cyberspace also have reinforced defenses. The concept here is not new. Defense can be layered based on priority of the asset to be protected. For cyberspace, these vital centers or key nodes (e.g., gateways, server hubs) must be defended commensurate with the access and content therein. Additionally, because cyberspace is multi-dimensional, assurance of authenticity and access must extend to nodes resident in the physical dimensions of land, sea, air, and space (e.g.. electrical power stations, buildings housing base servers, satellite command and control facilities, etc.). Although a standard minimum level of defense overall is essential, the opaqueness and vastness of the cyberspace domain precludes equal levels of protection when operating with limited resources. Moreover, the dynamic and regenerative feature of the cyberspace terrain allows for reconstitution of attacked sites online in cyberspace. To the extent that a redundant architecture and trained personnel are available, portions of

cyberspace that are denied access or whose content authenticity is suspected of compromise can be migrated to another vital center or node, such as another server physically located nearby or miles away.[9] Some quarantine measures would be required to ensure that malicious software has not been implanted.

Thus, perceiving cyberspace as a terrain comprised of linked IT hardware and software, whose interconnectivity is comprised of near-infinite electronic lines of communication between nodes and users reveals tractable physical and electronic dimensions. These lines of communication carry logistics and intelligence in electronic information format (e.g., ones and zeros that translate into funds, maintenance work orders, unit operational status, target descriptions). The IT hardware and software that powers it serves as the infrastructure. Connectivity permits these physically disparate networks to add to the cyberspace domain.

Given the sheer number of lines of communications in cyberspace, the cost of defense can be prohibitively high, even unrealistic, due to the limited battlespace awareness afforded by the opaque environment. Thus, expectations to secure every part or line of communication in cyberspace, even militarily relevant portions as a requirement for freedom of action is similar to trying to assert general control. If technologically feasible, it could result in impaired function due to severe security restrictions across the entirety of the DOD network. Leveraging cyberspace would be so cumbersome as to hinder or even impair operations that depended on its support capabilities. As network-centric warfare becomes more commonplace, there must be a balance such that operational mission accomplishment does not become enslaved under the tyranny of risk management. As Clausewitz presciently concluded,

[9] Kastenberg, "Georgia's Cyber Left Hook," 66-67.

chance is a part of the trinity of war.[10] No amount of defense or offense will eliminate risk in war. Part of the genius of great commanders is the ability to assess and mitigate risk without being paralyzed or overcome by it. In short, attempting to defend freedom of action over too large an expanse of cyberspace will undermine the overall intent of securing relevant portions of cyberspace, when needed.

As stated earlier, cost of entry is low since there are many options for access points into cyberspace where adversaries, upon achieving connectivity, can attempt to intercept or block friendly lines of communication. In maritime speak, cyberspace has many ports, some of which are strategic ports. In the geographic domains, they manifest as server hubs, relay stations, operations centers that monitor the status of base-wide, even region-wide networks. In cyberspace, Internet homepages are one manifestation of these ports. These can be construed as vital centers or key nodes and can be as significant to achieving domain control for cyberspace as they are for the geographic mediums. The strategic value of the servers and homepages are based on the level of information they contain and the distribution network they feed. Both defensive and offensive cyberspace operations can target efforts on these vital centers or key nodes.

Thus, in addition to being able to focus on vital centers or key nodes as a mechanism to defend freedom of action in cyberspace, economy of force is also a relevant principle for cyberspace control. In fact, it is a necessity unless there are unlimited resources. The territories across which the IT infrastructure supporting the DOD's use of cyberspace is too expansive and opaque to do point defense everywhere. Beyond the minimum level of protection, such as encryption, for access and authenticity of the majority of lines of

[10] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1984).

communications, military personnel should focus limited resources on reinforcing control over key nodes.

To reiterate, cyberspace superiority, as implied by DOD's dependencies upon it, has at minimum two requirements: assurance of authenticity and access. The freedom and ability to deny these two requirements will be foundational to controlling this new domain. If cyberspace can be construed as a warfighting domain that uniquely is a vast network of technologically finite lines of communication, its utility to the DOD and the US's adversaries may be approximated as being of similar relevance and value. Taking into account concerns of mirror-imaging, cyberspace is, at a minimum, both a data mine of informational resources and avenues for communication. Both the content and means of communication resident within cyberspace as a domain are of value.

With the ability to conduct activity in cyberspace, the military can take measures that deny adversaries freedom of action. Interestingly, the imperfections of the human world are passed onto this artificial domain, as well. System glitches and malfunctions have become such a norm when working with IT and cyberspace, the military must also be able to discern real attacks on freedom of action from unintentional causes. Both freedom of action and the ability to deny the same from adversaries can be complicated and assisted by the imperfections of cyberspace and the IT hardware and software infrastructure that allows activity in that domain.

Industrial capacity is a necessity for cyberspace superiority. Since cyberspace is a human creation, the hardware and software infrastructure are the means to access this domain and conduct activity there. Controlling the domain requires ensuring the integrity and security of the infrastructure. Just as the US and its Allies in World War II would not have used aircraft, tanks, ships, or other weapon systems manufactured by the Axis powers, the US must likewise be cautious of the IT infrastructure upon which its cyberspace activity depends. The

opportunity and dangers of sabotage are too great to be ignored. The network infrastructure offers both tangible and intangible areas for attack. It is a vulnerable and lucrative target system.

The opaque and technology-dependant nature of the cyberspace topography means minute or code-level changes are often imperceptible to the untrained layman or even human senses. Cyberspace superiority's requisite assurance for authenticity and access requires an IT infrastructure whose integrity is reasonably secure from deliberate tampering during research, development, production, and sustainment. Glitches and manufacturing and software coding errors are already inherent in this domain made by imperfect humans. The military should seek to reduce its IT-related problems by also protecting against deliberately-designed malfunctions, such as sabotage.

The US has both the resource potential and industrial capacity to produce indigenous and DOD-specific IT hardware and software. These two factors are recurring themes in controlling other domains. They can apply toward controlling cyberspace, as well. The DOD should require a cyberspace acquisition enterprise that is commensurate with those for other domains.

The artificial nature of cyberspace allows the US to establish protocols and systems that conform to government standards and requirements while still being interoperable, when necessary, with industry norms and structures. Reliance on commercial off-the-shelf (COTS) technology brings with it cost and availability advantages, but these may be outweighed by long-term risk. The military should decouple itself from the operating schemas of IT developed primarily for the civilian sector. The DOD can simultaneously reduce reliance on common operating schemas with which opponents are already familiar and partner with industry and academia to acquire hardware and software that enable the military to maintain a technological edge in cyberspace.

Where appropriate, COTS should remain an option, but it must not constitute the foundation of the military's cyberspace arsenal. Use of COTS technology must balance the inherent benefits of cost-effectiveness and instant availability with the operational risks of employing capabilities whose design specifications cannot be classified, are open source data, or worse, are wielded or improved upon by adversaries. The paradox of strategy does not need a helping hand.[11] The US military should not cede initiative and advantage in this technology-dependent domain by being over-reliant on COTS and failing to leverage its industrial capacity and resources through a cyberspace enterprise on par with other domains'.

Parallel operations within and across domains can also help attain cyberspace control. Extrapolating this salient commonality from control theories for other domains, a strategy to achieve cyberspace superiority must include more than military operations in cyberspace. In fact, it must include more than planning and activity in the domains that comprise the military front. There must be a deliberate military cradle-to-grave enterprise for cyberspace and its constituent IT hardware and software.

Additionally, since it is technology that enables (electronic) presence in cyberspace, the US has an inherent advantage given its information age capabilities. The artificiality of the domain allows those with sufficient knowledge and capability to set rules for their portions of cyberspace, to limit reliance on common operating schemas that hackers—freelance or otherwise—are already familiar with. Assurance of authenticity and controlled access requires a multi-layer defense, akin to Libicki's concept of castle defense.[12] Libicki also characterized cyberspace as having layers, describing them using linguistic parallels,

[11] Edward Luttwak, *Strategy : The Logic of War and Peace*, Rev. and enl. ed. (Cambridge, Mass.: Belknap Press of Harvard University Press, 2001).
[12] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 62.

such as physical, syntactic, and semantic.[13] The physical layer includes tangible elements, while the syntactic layer encompasses the programmatic languages and codes inherent to operating systems and applications.[14] The semantic level pertains to the information content of cyberspace.[15] Looking at cyberspace from Libicki's layered perspective offers other avenues for attaining and preserving domain control. Why should the DOD relegate its IT infrastructure, critical to national defense, to standards and capacities that are customized for commercial and private use? The DOD should implement military-specific physical, syntactic, and semantic layers for its cyberspace information systems.

This approach can deflect less sophisticated attackers by increasing the knowledge and logistical cost of infiltrating or defeating US military cyberspace systems. Complex cyber attacks, while more harmful, also often require more knowledge and an IT infrastructure and logistics that must be state-sponsored, hijacked, or a combination thereof. The elaborate planning and technical skills required would deter swaths of would-be attackers.

Reducing the pool of potential assailants by increasing the cost of intellectual capital and logistics would also aid attribution of attack. The cloak of anonymity that may embolden attacks via cyberspace is now less assured, serving to deter those whose risk tolerance is influenced by the probability the US military will identify them as culprits. It would be foolish, however, to expect to deter or to defend successfully against every instance of cyber attack. Nonetheless, defense takes many forms, and in aggregate, the number of attackers deterred reduces the number that must be actively countered.

Dynamic and regenerative, cyberspace warfare also requires persistence to maintain battlespace awareness of status of US,

---

[13] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 8-9.
[14] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 8-9, 24-25.
[15] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 24-25.

adversary, and gray systems and activity. Adaptive persistence and parallel operations are required to defend, deny, and disrupt freedom of action in cyberspace. The DOD must be ready to give chase across many lines of communications and vital centers. More importantly, the difficulty and time required to be able to lead-turn an adversary must not be underestimated. Adequate intelligence of network architectures and adversary personnel skills and trademark TTPs will be as fundamental to cyberspace as they are to the geographic domains.

Chapter 5

Conclusions

There has also been reluctance, since the end of the Cold War, to undertake a serious review of strategy because this could involve questioning some very comfortable assumptions about the place of the United States in the world and how other nations view us. We are not indispensible, a hegemon, or unchallenged, and the evolution of cyberspace clearly reflects this.

Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity

Yes, I think we need a cyber Monroe Doctrine.

Lieutenant General Keith Alexander

Cyberspace is still relatively new territory in warfare's history. The way to the cyberspace superiority Holy Grail is a multifaceted approach, requiring coordinated, parallel and persistent efforts across all domains in which cyber hardware and software infrastructure exists. As the DOD assesses its cyberspace dependencies and vulnerabilities, the necessity for ability to control the domain, so that the military can effectively defend vital national interests in this and other domains, has been declared. The DOD, however, will require a cyberspace enterprise that is commensurate with those that support other warfighting domains. Cyberspace control will be neither cheap nor simple in economic and intellectual terms. Controlling cyberspace as a military domain is a new challenge that demands continuing investment in critical thought. Assessing the right questions, especially those at the foundation of its strategic assumptions, is essential.

This thesis examined whether cyberspace can be controlled in like manner to existing mediums. Cyberspace can be controlled in ways analogous to land, sea, and air domains. The US military, however,

must be careful that the momentum of reorganization for cyberspace operations does not cause it to gloss over key issues. The military's strategy development for cyberspace superiority must be deliberate rather than fortuitous.

Cyberspace control is not a Holy Grail. A brief survey of classical control theories for the land, maritime, and air domains, with the intent of identifying the basic framework and its key areas of emphasis, revealed several common elements in domain control. Strategies by theorists, such as Halford Mackinder and Nicholas Spykman for land-centric theories; Alfred Thayer Mahan and Julian Corbett for sea control theories; and William "Billy" Mitchell and J. C. Slessor for the air domain, can inform present-day and future cyberspace theorists and war planners. Given the nature of the cyberspace medium and the denominators common to controlling other domains, the US can gain and maintain cyberspace superiority. Denominators common across the classical control theories for air, land, and sea exist and are applicable to cyberspace's attributes as a dimension of war. The US, however, must be careful not to under or overreach in its grab for the Holy Grail.

Implications

Although the concept and acceptance of cyberspace and warfare in this domain is relatively new when juxtaposed with its land, sea, and air contemporaries, cyber warfare is not bereft of historical antecedents upon which to build a control strategy. Flexibility in being able to learn from the past theories of control and to adapt them to this newly contested domain will be the key to the quest for the Holy Grail of controlling the cyberspace domain.

As important, in the foreseeable future, debate will and must continue over aspects of cyberspace. Society will encounter the socio-political-economic-military and organizational struggle that befell, and still constrains, space exploitation and control. Over two decades after

the creation of Air Force Space Command, space scholars such as John Sheldon, still had to advise that "Space is a unique strategic environment, and air and sea power analogies that claim it for their own are overblown. Space has its own unique terrain and geography…that must be understood on their own terms, and which dictate the operational parameters and tactics of space power."[1] The same likewise can be applied to cyberspace. When exploring new dimensions of war, growing pains can persist for decades, even centuries. While these types of obstacles slow progress, they should not discourage continued discourse and study. They should be expected and harvested for the lessons they may offer in order to achieve progress.

Thus, to expect full comprehension and resolution of issues at this relatively early juncture in cyberspace history, such that a robust cyberspace control theory may be crafted, is naïve. Although strategic theories should outlast tactics, which are more affected by technological changes, there is nonetheless room for intellectual growth throughout the emerging cyberspace enterprise. The character of conflict in this domain has neither matured nor reached a temporary plateau.

Regardless, the US military, especially its Air Force, has already decided to accept these new concepts, in order to better focus limited resources on crafting a deliberate approach to resolving and anticipating cyber-related challenges. Thus, to the DOD's credit, the military has trekked into this new frontier while it is still cognitively grappling with the definitions and boundaries for its new cyber vocabulary and concepts. The maelstrom of debate continues. Nonetheless, there is sufficient, albeit limited knowledge, of cyberspace that renders this medium tractable for the military to conclude it can discern how to control it.

[1] John B. Sheldon, "Reasoning by Strategic Analogy: Classical Strategic Thought and the Foundations of a Theory of Space Power," (Reading: University of Reading, 2005), 304.

As significantly, control of the cyberspace domain can be informed by classical control theories. The cyberspace domain has merely added another dimension to the character of war. Author David Lonsdale accurately concludes that while the nature of war remains as Carl von Clausewitz described, the information age and its attendant fifth dimension have amended war's character.[2] As a result, any country that connects to cyberspace is a potential participant in cyber warfare.

At the time of this writing, in one month alone, both Kyrgyzstan and Britain suffered cyber attacks. While the specifics on the attackers and their agenda may never truly be known, the media highlighted the two events. They were additional data points for the growing phenomenon of cyber warfare. From a military perspective, these events supported Clausewitz's assertion that war—cyber or otherwise—still serves political ends.[3] The nature of warfare and its purpose remain intact despite the advent of cyber warfare and cyberspace as a warfighting medium.

The incident in Kyrgyzstan took the form of "denial-of-service attacks [targeting the country's two main Internet service providers and] managed to shut down more than 80 percent of Kyrgyzstan's bandwidth."[4] A pattern of implicit encouragement of cyber attacks, against Georgia in 2008 and against Estonia in 2007, paints Russia as the likeliest source, or sponsor, of the attacks on Kyrgyzstan. "The *Wall Street Journal* now reports that the cyber-attack may have been orchestrated by a Russia-based 'cyber militia,' although it provides few additional details about who, exactly, was responsible."[5] Is it reasonable

---

[2] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 202.
[3] Carl von Clausewitz, Michael Eliot Howard, and Peter Paret, *On War* (Princeton, N.J.: Princeton University Press, 1976), 87.
[4] Nathan Hodge, "Russian 'Cyber Militia' Takes Kyrgyzstan Offline?," *Wired Blog Network, Dangerroom* (January 28, 2009), http://blog.wired.com/defense/2009/01/cyber-militia-t.html. Accessed January 30, 2009.
[5] Hodge, "Russian 'Cyber Militia' Takes Kyrgyzstan Offline?."

to assume that one of the early acts of future warfare will now include inciting computer-savvy nationalist sympathizers to generate cyber activity against the government's antagonist or target?[6] The Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency reports, "Exploiting vulnerabilities in cyber infrastructure will be part of any future conflict. If opponents can access a system to steal information, they can also leave something behind that they can trigger in the event of conflict or crisis. Porous information systems have allowed opponents to map our vulnerabilities and plan their attacks…. We should expect that exploiting vulnerabilities in cyber infrastructure will be part of any future conflict."[7] The opportunities for these kinds of attacks, ad hoc or pre-planned, by civilian sympathizers or cyber-mercenaries, preceding or during broader conflicts are more than conjecture.

The grand strategic relevance becomes apparent as the possibility that the cyber attack was conducted as a means to political ends emerges. "Several commentators have speculated that the attack is meant to thwart Kyrgyzstan's embattled political opposition—which depends on the Internet to organize—or to pressure Kyrgyzstan's government, which hosts a US airbase outside of the capital, Bishkek."[8]

Meanwhile, the cyber attack on Britain appears as another data point for the rising tide of direct attacks against military forces. The British Ministry of Defence (MOD) had to defend against an email worm that redirected "e-mails from multiple Royal Air Force facilities to computers inside Russia" and reportedly drove "MOD officials to shut down all e-mail for a period … ."[9] Although no physical damage resulted,

---

[6] Author discussion with Dr. John B. Sheldon, February 2009.
[7] (CSIS) Center for Strategic and International Studies, "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency," (2008), 13.
[8] Hodge, "Russian 'Cyber Militia' Takes Kyrgyzstan Offline?."
[9] Sean Gallagher, "British Military Hit with Cyberattacks," *Defense Systems* (January 22, 2009), http://defensesystems.com/blogs/forward-observer/2009/01/british-military-hit-by-cyber-attacks.aspx?s=ds_280109. Accessed January 30, 2009.

this cyber attack constituted an assault on military forces, aimed at British lines of communications and intelligence collection. Additionally, the "attack comes on the heels of a malware attack on the US Department of Defense's networks late last year.... [that] led to the...ban on removable media such as USB 'thumb drives,' which were an alleged culprit in the attacks."[10] For the attacker, these cyber attacks on the British MOD and US DOD align with Sun Tzu's tenets regarding indirect approaches to influencing an adversary's behavior, the importance of intelligence collection, and observation of response patterns.[11]

The DOD's vision for the military's role in cyberspace is "to develop cyberspace capability that provides global situational awareness of cyberspace, US freedom of action in cyberspace, the ability to provide warfighting effects within and through cyberspace, and, when called upon, provide cyberspace support to civil authorities."[12] The DOD also purports to follow an "approach to cyberspace [that] must remain flexible as our understanding of the domain continues to mature, and as US, alliance, coalition partners, and adversary capabilities to operate in cyberspace increase."[13] In fact, as of May 2009, the leadership of the National Security Agency, a significant stakeholder in the US's cyberspace establishment, raised the bold notion that "the United States should develop a policy to protect cyberspace based on the nearly 200-year-old Monroe Doctrine, which declared that any effort to interfere with nations in the Western Hemisphere would be viewed as 'dangerous to our peace and safety.'"[14] Rhetoric and reality will both be improved, in terms of national credibility, when assertions and the assumptions upon which

---

[10] Gallagher, "British Military Hit with Cyberattacks."
[11] Sun Tzu, *The Illustrated Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, Inc., 2005), 152.
[12] Defense, "Quadrennial Review Report," 14.
[13] Defense, "Quadrennial Review Report," 18.
[14] Bob Brewin, "NSA Director Calls for a Cyberspace Monroe Doctrine," *NextGov: Technology and the Business of Government* (May 6, 2009), http://www.nextgov.com/site_services/print_article.php?StoryID=ng_20090506_4087. Accessed May 14, 2009.

they are predicated, are informed by past evidence and by theories that were already vetted across similar, though distinct, domains.

Bibliography

Brewin, Bob. "NSA Director Calls for a Cyberspace Monroe Doctrine." *NextGov: Technology and the Business of Government* (May 6, 2009), http://www.nextgov.com/site_services/print_article.php?StoryID=ng_20090506_4087.

Center for Strategic and International Studies, (CSIS). "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." 2008.

Clausewitz, Carl von. *On War*. Translated by Michael Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1984.

Clausewitz, Carl von, Michael Eliot Howard, and Peter Paret. *On War*. Princeton, N.J.: Princeton University Press, 1976.

Corbett, Julian S. *Some Principles of Maritime Strategy*. Edited by Eric J. Grove, Classics of Sea Power. Annapolis, MD: Naval Institute Press, 1988.

Defense, Department of. "Quadrennial Roles and Missions Review Report." January 2009.

Gallagher, Sean. "British Military Hit with Cyberattacks." *Defense Systems* (January 22, 2009), http://defensesystems.com/blogs/forward-observer/2009/01/british-military-hit-by-cyber-attacks.aspx?s=ds_280109.

Grant, Rebecca. "Victory in Cyberspace." Arlington, VA: Air Force Association, 2007.

Gray, Colin S. *Modern Strategy*. Oxford: Oxford University Press, 1999.

Hodge, Nathan. "Russian 'Cyber Militia' Takes Kyrgyzstan Offline?" *Wired Blog Network, Dangerroom* (January 28, 2009), http://blog.wired.com/defense/2009/01/cyber-militia-t.html.

Joint Chiefs of Staff, Chairman. "The National Military Strategy for Cyberspace Operations (U)." (Secret) Information extracted is unclassified.

Joint Chiefs of Staff, Vice Chairman. "Definition of Cyberspace Operations Action Memo for Deputy Secretary of Defense." September 29, 2008.

Kastenberg, Stephen W. Korns and Joshua E. "Georgia's Cyber Left Hook." *Parameters* Winter 2008-2009 (2009).

Kennedy, Paul M. *The Rise and Fall of British Naval Mastery*. Malabar, FL: Robert E. Krieger Publishing Company, 1982.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. London: Frank Cass, 2004.

Lord, William T. "USAF Cyberspace Command: To Fly and Fight in Cyberspace." *Strategic Studies Quarterly* (Fall 2008).

Luttwak, Edward. *Strategy : The Logic of War and Peace*. Rev. and enl. ed. Cambridge, Mass.: Belknap Press of Harvard University Press, 2001.

Mackinder, Halford J. *Democratic Ideals and Reality: A Study in the Politics of Reconstruction*. New York: Henry Holt and Company, 1919.

———. "The Geographic Pivot of History." In *The Scope and Methods of Geography and the Geographical Pivot of History: Reprinted with an Introduction by E.W. Gilbert*. London: William Clowes and Sons, Limited, 1951.

Mahan, Alfred T. *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*. Edited by John B. Hattendorf, Classics of Sea Power. Annapolis, MD: Naval Institute Press, 1991.

Mitchell, William. *Winged Defense : The Development and Possibilities of Modern Air Power Economic and Military*. Mineola, N.Y.: Dover Publications, 2006.

Rattray, Gregory. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Rittel, Horst, and Melvin Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4 (1973).

Secretary of Defense, Deputy. "The Definition of 'Cyberspace'." May 12, 2008.

Sheldon, John B. "Reasoning by Strategic Analogy: Classical Strategic Thought and the Foundations of a Theory of Space Power." Reading: University of Reading, 2005.

Slessor, John Cotesworth. *Air Power and Armies*. London: Oxford university press : Reprint by AMS Press New York, 1936.

Spykman, Nicholas J. *The Geography of the Peace*. New York: Harcourt, Brace and Company, 1944.

Sun Tzu. *The Illustrated Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, Inc., 2005.

Wylie, Joseph. *Military Strategy: A General Theory of Power Control*, Classics of Sea Power. Annapolis, MD: Naval Institute Press, 1989.